

ABSTRACT

To protect a private cryptographic key, two values are derived. The two values together can reconstruct the key. One value is sent to a server and deleted from the local machine. The other value is held by the local machine. To use the key, the user will enter a password, which will be used to authenticate the user to the server, and retrieve the value from the server. The password is also used to unlock the value held by the local machine. The private cryptographic key is thus protected against brute force password attacks without changing the behavior of the user.